REMARKS

In the Office Action, the Examiner noted that claims 20-22 are pending in the application and that claims all claims (20-22) are rejected. In this Amendment claim 20 is amended, no claims are cancelled and claims 23-44 are added. Thus, claims 20-44 are pending in this application. Applicant submits that no new matter has been introduced into the application. In this regard, the new claims and amendments are fully supported by the original specification and drawings at, for example, pages 56-57.

The rejections are respectfully traversed below.

Rejections Under 35 USC § 103(a)

Claims 20-22 stand rejected under 35 USC § 103(a) as being unpatentable over U.S. Patent No. 5,706,047 (hereinafter Lentz) in view of U.S. Patent No. 5,313,193 (hereinafter Dubois).

These rejections are respectfully traversed for the reasons discussed below.

The present invention is directed to a technique for authenticating a data media in order to prevent unauthorized copying of the media. More particularly, at least one predetermined tracing substance (e.g., a predetermined concentration of at least one isotope) is impregnated within the media. In order to read data stored on the media, the media must be authenticated by detecting the tracing substance. This tracing substance takes the form of, for example, a powder, which may be dispersed or pressed into the media during its manufacturing process (see, FIG. 7). The tracing substance is therefore detectable in any portion of the media, including a data area (i.e., an area of the media that stores data). As such, it is practically impossible to remove the tracing substance from the media. This feature is important because it prevents an unauthorized

user from simply destroying a portion of the media to remove the tracing substance. Indeed, each of the independent claims rejected by the Examiner specifically recites a combination of elements including **"wherein at least a data area of said media is impregnated with at least one predetermined tracing substance"**, and detecting **"the at least one security marking in said data area of said data media"**.

In contrast, Lentz discloses a storage media that has an identification code imbedded in the mirror area (see, mirror area 52 in FIG. 5) of the media. This mirror area of the media does not store data and is, therefore, not a data area. Lentz states:

> The mirror area 52 has a storage layer associated therewith but does not have data embedded therein and, therefore, has a mirror-like appearance.

The identification code of Lentz is created by focusing high intensity laser radiation (col. 4, lines 13-14) onto mirror area 52 to create a number of physical disruptions (col. 4, lines 54-56; FIG. 5). These disruptions, if implemented in a data area, would destroy any data stored therein. Thus, the disruptions must be created in mirror area 52. Importantly, by embedding the identification code in a single location on a media (i.e., mirror area 52), an unauthorized user would destroy the mirror area of the media and remove the identification code, thereby circumventing any of its security features.

As mentioned above, to embed the identification code of Lentz anywhere else but in the mirror area 52 would serve to destroy the data area, and thus render the device of Lentz inoperable. In particular, the identification code of Lentz is created by disrupting a reflector layer 25 of the media (see, FIG. 4a and 4b). The disruption is used to 'write' machine readable code or human readable markings (col. 4, lines 23 and 54-56). Creating the disruptions in the data area would destroy valuable data storage space. Thus, the disruption is created in mirror area 52, because no data is stored there.

Without conceding that Lentz or Dubois discloses any of the elements of the present invention, it is clear that Lentz does not teach or disclose the combination, including at least "**a data area impregnated with at least one predetermined tracing substance**". Just as important, Lentz does not teach or disclose detecting "**the at least one security marking in said data area of said data media**".

None of the other cited references, including Dubois, do anything to address the above-noted deficiencies of Lentz in a manner that teaches or suggests the combination of features of the present invention. In particular, none of the other references of record disclose, alone or in combination, "**a data area impregnated with at least one predetermined tracing substance**" or detecting "**the at least one security marking in said data area of said data media**". Dubois, for example, was cited for its teaching of the use of radioisotopes as a detectable substance. However, Dubois makes no mention of using these radioisotopes in a data area of a data media. In fact, Dubois teaches that a portion of the object to be marked must be removed via **etching** (col. 3, line 30) to implant the radioisotope (see, e.g., FIG. 2d). Thus, modifying Lentz with the teachings of Dubois would either result in: 1) the destruction of data storage space or 2) the creation of markings in an area that is not used to store data or a nondata area (e.g., similar to the mirror area 52 of Lentz). In any event, it is clear that Dubois and the other cited references of record provide no disclosure or suggestion that would have motivated a person of ordinary skill in the art to modify Lentz, or to make any combination of the references of record in such a manner as to result in or otherwise render obvious the combination of features, as now recited by the limitations in the independent claims, when each claim is interpreted as a whole.

Accordingly, the Applicant submits that none of the references cited by the Examiner shows or suggests the combination of features, as now recited by the limitations in the

independent claims, of the present invention.

Referring now to the claims where the specific combination of elements is asserted to be patentable over the prior art when interpreted as a whole, independent claim 20 recites a combination of features directed to a "method for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media". As recited, the method comprises the steps of "detecting the at least one security marking in said data area of said data media". Claim 20 also recites "authenticating said data media responsive to said detecting step . . . using the at least one security marking". Finally, claim 20 recites "outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said authenticating step". Accordingly, the combination of features of independent claim 20, when interpreted as a whole, is submitted to patentably distinguish over the references of record.

Claim 26 is directed to the combination of a "system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media". As recited, the

system comprises "a sensor that detects the presence of the at least one security marking in said data area of said data media". Claim 26 also recites "a processor that is capable of authenticating said data media using the at least one security marking". Finally, claim 26 recites " a playback device that is capable of outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated." Accordingly, the combination of features of independent claim 26, when interpreted as a whole, is submitted to patentably distinguish over the references of record.

In addition, claim 33 is directed to the combination of a "system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media". Claim 33 recites means for detecting the at least one security marking in said data area of said data media". Claim 33 also recites "means for authenticating said data media responsive to said means for detecting using the at least one security marking". Finally, claim 33 recites "means for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said means for authenticating." Accordingly, the combination of features of independent claim 33, when interpreted as a whole, is submitted to patentably distinguish over the references of record.

Also, claim 40 is directed to the combination of a "computer readable medium for

authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media". As recited, the computer readable medium comprises "computer readable instructions for detecting the at least one security marking in said data area of said data media". Claim 40 also recites "computer readable instructions for authenticating said data media responsive to said computer readable instructions for detecting using the at least one security marking". Finally, claim 40 recites "computer readable instructions for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated." Accordingly, the combination of features of independent claim 40, when interpreted as a whole, is submitted to patentably distinguish over the references of record.

Therefore, it is respectfully submitted that the independent claims of the present invention, as well as the claims depending therefrom, are clearly allowable over the prior art of record.

In addition, the present invention provides benefits over the cited references of record. For example, as discussed above, in the present invention it is not possible to circumvent the security features without destroying data. In Lentz, a copyist may remove a security marking by destroying a mirror area without damaging any data, thereby circumventing its security features. For these reasons as well, Applicant respectfully submits that the claims are patentable over the references of record.

Dependent Claims

The dependent claims of the present application are further distinguishable over the references of record for their own additional features as well. For example, claims 25, 31, 38, and 43 indicate that the security marking of the present invention must be detected from within a data area of the media. None of the references cited by the Examiner shows or suggests this feature in combination with the remaining features of the independent claims. Therefore, Applicant respectfully submits that the dependent claims of the present invention are patentable, for their own additional reasons, over the references of record.

For all of the reasons discussed above, withdrawal of the current rejections is respectfully requested.

CONCLUSION

Applicant respectfully submits that, as described above, the cited prior art does not show or suggest the combination of features recited in the claims. Applicant does not concede that the cited prior art shows any of the elements recited in the claims. However, Applicant has provided specific examples of elements in the claims that are clearly not present in the cited prior art.

Applicant strongly emphasizes that one reviewing the prosecution history should not interpret any of the examples Applicant has described herein in connection with distinguishing over the prior art as limiting to those specific features in isolation. Rather, Applicant asserts that it is the combination of elements recited in each of the claims, when each claim is interpreted as

a whole, which is patentable. Applicant has emphasized certain features in the claims as clearly not present in the cited references, as discussed above. However, Applicant does not concede that other features in the claims are found in the prior art. Rather, for the sake of simplicity, Applicant is providing examples of why the claims described above are distinguishable over the cited prior art.

Applicant wishes to clarify for the record, if necessary, that the claims have been amended to expedite prosecution. Moreover, Applicant reserves the right to pursue the original subject matter recited in the present claims in a continuation application.

Any narrowing amendments made to the claims in the present Amendment are not to be construed as a surrender of any subject matter between the original claims and the present claims; rather merely Applicant's best attempt at providing one or more definitions of what the Applicant believes to be suitable patent protection. In addition, the present claims provide the intended scope of protection that Applicant is seeking for this application. Therefore, no estoppel should be presumed, and Applicant's claims are intended to include a scope of protection under the Doctrine of Equivalents.

For all the reasons advanced above, Applicant respectfully submits that the rejections have been overcome and should be withdrawn.

For all the reasons advanced above, Applicant respectfully submits that the Application is in condition for allowance, and that such action is earnestly solicited.

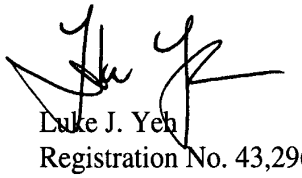
AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this Amendment, or credit any overpayment to deposit account no. 08-0219.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to deposit account no. 08-0219.

Respectfully submitted,

HALE AND DORR LLP



Luke J. Yeh
Registration No. 43,296

1455 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
TEL 202.942.8495
FAX 202.942.8484
Date: 3/3/03
LJY:sgs/110267-201 US3
203093v1

Attachment A
(amendments indicated with brackets and underlines)

20. (Once Amended) A method for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said method comprising the steps of:

(a) detecting the at least one security marking in said data area of said data media;

(b) authenticating said data media responsive to said detecting step (a) using the at least one security marking; and

(c) outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said authenticating step (b).

21. The authenticating method according to claim 20, and further including the step of authenticating said data media via at least two different security markings, each of which successively must be authenticated before said data is finally output via said outputting step (c).

22. The authenticating method according to claim 20, and further including the step of authenticating said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

23. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

24. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

25. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises reading information from said data area of said data media.

26. (New) A system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said system comprising:

a sensor that detects the presence of the at least one security marking in said data area of said data media;

a processor that is capable of authenticating said data media using the at least one security marking; and

a playback device that is capable of outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated.

27. (New) The system according to claim 26, wherein said processor authenticates said data media via at least two different security markings, each of which successively must be authenticated before said data is finally outputted.

28. (New) The system according to claim 26, wherein said processor authenticates said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

29. (New) The system according to claim 26, wherein said sensor detects the at least one security marking by detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

30. (New) The system according to claim 26, wherein said sensor detects the at least one security marking by using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

31. (New) The system according to claim 26, wherein said sensor detects the at least one security marking by reading information from said data area of said data media.

32. (New) The system according to claim 26, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.

33. (New) A system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said system comprising:

means for detecting the at least one security marking in said data area of said data media;

means for authenticating said data media responsive to said means for detecting using the at least one security marking; and

means for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said means for authenticating.

34. (New) The system according to claim 33, wherein said means for authenticating authenticates said data media via at least two different security markings, each of which successively must be authenticated before said data is finally outputted.

35. (New) The system according to claim 33, wherein said means for authenticating authenticates said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

36. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

37. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

38. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for reading information from said data area of said data media.

39. (New) The system according to claim 33, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.

40. (New) A computer readable medium for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said computer readable medium comprising:

computer readable instructions for detecting the at least one security marking in said data area of said data media;

computer readable instructions for authenticating said data media responsive to said computer readable instructions for detecting using the at least one security marking; and

computer readable instructions for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated.

41. (New) The computer readable medium according to claim 40, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

42. (New) The computer readable medium according to claim 40, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

43. (New) The computer readable medium according to claim 40, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for reading information from said data area of said data media.

44. (New) The computer readable medium according to claim 40, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.

Attachment B
(complete set of the claims as amended)

20. (Once Amended) A method for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said method comprising the steps of:

(a) detecting the at least one security marking in said data area of said data media;

(b) authenticating said data media responsive to said detecting step (a) using the at least one security marking; and

(c) outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said authenticating step (b).

21. The authenticating method according to claim 20, and further including the step of authenticating said data media via at least two different security markings, each of which successively must be authenticated before said data is finally output via said outputting step (c).

22. The authenticating method according to claim 20, and further including the step of authenticating said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

R 1.26

25. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

26
~~24~~. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

27
~~25~~. (New) The authenticating method according to claim 20, wherein said step of detecting the at least one security marking comprises reading information from said data area of said data media.

28
~~26~~. (New) A system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said system comprising:

a sensor that detects the presence of the at least one security marking in said data area of said data media;

a processor that is capable of authenticating said data media using the at least one security marking; and

a playback device that is capable of outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated.

29 28
~~27~~. (New) The system according to claim ~~26~~, wherein said processor authenticates said data media via at least two different security markings, each of which successively must be authenticated before said data is finally outputted.

30 28
~~28~~. (New) The system according to claim ~~26~~, wherein said processor authenticates said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

31 28
~~29~~. (New) The system according to claim ~~26~~, wherein said sensor detects the at least one security marking by detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

32 28
~~30~~. (New) The system according to claim ~~26~~, wherein said sensor detects the at least one security marking by using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

33 28
~~31~~. (New) The system according to claim ~~26~~, wherein said sensor detects the at least one security marking by reading information from said data area of said data media.

Cont'

34 28
~~32~~. (New) The system according to claim ~~26~~, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.

35
~~33~~. (New) A system for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said system comprising:

means for detecting the at least one security marking in said data area of said data media;

means for authenticating said data media responsive to said means for detecting using the at least one security marking; and

means for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated by said means for authenticating.

36 35
~~34~~. (New) The system according to claim ~~33~~, wherein said means for authenticating authenticates said data media via at least two different security markings, each of which successively must be authenticated before said data is finally outputted.

37 35. (New) The system according to claim 33, wherein said means for authenticating authenticates said data media over a plurality of interconnected computer networks comprising at least one of a local network, global network and Internet.

38 36. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

39 37. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

Bart

40 38. (New) The system according to claim 33, wherein said means for detecting the at least one security marking comprises means for reading information from said data area of said data media.

41 39. (New) The system according to claim 33, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.

42 40. (New) A computer readable medium for authenticating a data media storing data in order to prevent at least one of piracy, unauthorized access and unauthorized copying of said data media, wherein at least a data area of said media is impregnated with at least one predetermined tracing substance including a predetermined concentration of at least one of an isotope, a plurality of isotopes and a plurality of stable isotopes, to form at least one security marking used for at least one of tracking and authenticating said data media, said computer readable medium comprising:

computer readable instructions for detecting the at least one security marking in said data area of said data media;

computer readable instructions for authenticating said data media responsive to said computer readable instructions for detecting using the at least one security marking; and

computer readable instructions for outputting said data stored on said data media as at least one of audio, video, audio data, video data and digital data substantially free of said at least one security marking when the data media has been successfully authenticated.

43 ~~41~~. (New) The computer readable medium according to claim 42 ~~40~~, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for detecting at least one of a transparent oxide of at least one of a silicate, a lead dioxide, tin, cadmium 12 and iridium 5, or combination thereof.

B2 Cont'd

44 ~~42~~. (New) The computer readable medium according to claim 42 ~~40~~, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for detecting using at least one of mass spectrometry, neutron absorption and neutron spectrometry techniques.

45 ~~43~~. (New) The computer readable medium according to claim 42 ~~40~~, wherein said computer readable instructions for detecting the at least one security marking comprises computer readable instructions for reading information from said data area of said data media.

46 ~~44~~. (New) The computer readable medium according to claim 42 ~~40~~, wherein said outputted at least one of said audio, video, audio data, video data and digital data is stored in said data area of said data media.